UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

GUAVA, LLC, Plaintiff, v. JOHN DOE, Defendant.	Civil Action No.: **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Guava, LLC ("Plaintiff"), by and through its undersigned counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as follows:

NATURE OF THE CASE

1. Plaintiff files this action for computer fraud and abuse and civil conspiracy, arising from unlawful computer-based breaches and data distribution. By this action, Guava seeks, *inter alia*, compensatory damages, injunctive relief and attorney's fees and costs.

PARTIES

2. Plaintiff is a limited liability company that operates protected computer systems, including computer systems accessible throughout Minnesota.

3. Defendant's actual name is unknown to Plaintiff. Instead, Defendant is known to Plaintiff only by an Internet Protocol ("IP") address assigned to Defendant. An IP address is a number assigned to devices, such as computers, that are connected to the Internet. In the course of monitoring individuals seeking unauthorized access to Plaintiff's websites, Plaintiff's agents observed unlawful reproduction and distribution occurring over IP address 24.197.177.11. On information and belief, the IP address was assigned to Defendant by his or her Internet Service

Provider. Plaintiff cannot ascertain Defendant's actual identity without limited expedited discovery.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to the Federal Computer Fraud and Abuse Act, codified at 18 U.S.C. §§ 1030, *et seq.*, (the "CFAA"), and pursuant 28 U.S.C. § 1331 (actions arising under the laws of the United States). This Court has supplemental jurisdiction over the conspiracy claim because it is so related to Plaintiff's CFAA claim, which is within this Court's original jurisdiction, that the claims form part of the same case and controversy under Article III of the United States Constitution.

5. This Court has personal jurisdiction over the Defendant because, upon information and belief, he resides in the State of Minnesota. Plaintiff used geolocation technology to trace the IP address of Defendant to a point of origin within the State of Minnesota. Geolocation is a method for ascertaining the likely geographic region associated with a given IP address at a given date and time. Although not a litmus test for personal jurisdiction, the use of geolocation gives Plaintiff good cause for asserting that personal jurisdiction is proper over Defendant.

6. Venue is properly founded in this Court pursuant to 28 U.S.C. §§ 1391(b) and 1400(a) because Defendant resides in this District, may be found in this District, or a substantial part of the events giving rise to the claims in this action occurred within this District.

BACKGROUND

7. The Internet has made nearly unlimited amounts of information and data readily available to anyone who desires access to it. Some of this information and data is private, available only to those who have a lawful access to it. Owners attempt to protect this private

information through the use of password authentication systems. Unfortunately, this safety device does not ensure that information remains protected from unauthorized access.

8. Hacking is the act of gaining access without legal authorization to a computer or computer system. This is normally done through the use of special computer programming software that "cracks" the password. This password cracking software repeatedly attempts to guess a password until the correct password is ascertained. The software can attempt a great number of passwords in a short period of time, sometimes even a million per second, making this type of software very efficient at obtaining a password. Individuals that utilize this type of software are called hackers.[1] Hackers employ various other means to gain unauthorized access to data such as identifying information exploitable flaws in database codes.

9. Once a password is obtained, the hacker has unauthorized access to the protected information as long as the password remains valid. Sometimes a hacker will post the hacked username and password on a hacked username/password website, making it available to the members or visitors of that website. The posting hacker may even charge individuals for use of the hacked username and password and make a profit off of the loss and harm that he or she has caused to the website owner or users. There are not necessarily any limits on how often or by how many people a password can be used, so a single hacked username and password can potentially allow unauthorized access to significant numbers of individuals.

[1] The technical definition of a "hacker" is actually much broader and includes anyone who modifies a computer system to accomplish a goal—whether authorized or not (very similar to a computer programmer). A "cracker" is the technically correct definition of someone who gains unauthorized access to a computer. However, the common popular definition of "hacking" is generally understood to be that of a "cracker." In this document, any references to "hacker" or "hacking" will refer to, and be indistinguishable from, the common definitions of "cracker" or "cracking."

FACTUAL ALLEGATIONS

10. Plaintiff is the owner and operator protected computer systems, including protected computer systems that are accessible in Minnesota.

11. Plaintiff invests significant capital in maintaining and operating its websites. Plaintiff makes the websites available only to those individuals who have been granted access to Plaintiff's website (i.e., paying members). This access is given to members of the Plaintiff's websites who sign-up and pay a fee to access Plaintiff's websites. Access to this protected information is protected by a password assigned to each individual member.

12. Plaintiff's computer systems are regularly targeted by hackers who wish to gain unauthorized access to Plaintiff's valuable information.

13. When hackers successfully breach Plaintiff's protected systems, they and their fellow co-conspirators take, and may distribute, the misappropriated information in a highly-coordinated manner to their fellow Internet-based co-conspirators.

14. The process of probing Plaintiff's defenses, breaching Plaintiff's protected systems and distributing misappropriated information is an ongoing problem that continues to this day.

15. On information and belief, security systems to prevent hacking are not infallible, and can be successfully bypassed through the efforts of savvy hackers, allowing such hackers to access the systems that a client, like Plaintiff, attempts to protect.

16. On information and belief, Defendant belongs to a hacking community where hacked usernames and passwords are passed back and forth among members. Members of this community work together to ensure that the members have access to normally inaccessible and unauthorized areas of the Internet. The series of transactions in this case involved accessing and

sharing hacked username and passwords over the Internet and using the hacked username and passwords to access Plaintiff's website and private systems. Defendant participated with other hackers in this community, in order to disseminate the hacked usernames and passwords, and intentionally acted to access Plaintiff's website and systems through the use of hacked usernames and passwords.

17. Defendant gained unauthorized access to Plaintiff's private websites. Defendant used a hacked username and password to gain unlawful access to the member's sections of Plaintiff's websites. Through these hacked usernames and passwords Defendant accessed Plaintiff's systems as though Defendant was a paying member. Further, Defendant downloaded Plaintiff's private information, which is not available to members, and disseminated that information to other unauthorized individuals.

18. Since Defendant accessed the website through hacked usernames and passwords, Defendant would not have been required to provide any identifying personal information, such as his or her true name, address, telephone number or email address.

19. Plaintiff retained a forensic computer consultant to identify IP addresses associated with hackers who use hacked usernames and passwords and the Internet to access Plaintiff's private websites and systems.

20. The forensic evidence gathered on behalf of Plaintiff identified that IP address 24.197.177.11 was used for hacking, unauthorized access, and/or password sharing activity on Plaintiff's websites.

21. In addition to logging Defendant's IP address, Plaintiff obtained other important information, such as the specific websites that were unlawfully accessed and the files that were downloaded during that unauthorized access.

22. Once Defendant's IP address and dates and time of unlawful access were ascertained, Plaintiff used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP address and the putative location of those IP address used to perpetrate the hacking. Furthermore, on information and belief, Defendant was in control of the IP address during all relevant times.

COUNT I – COMPUTER FRAUD AND ABUSE

23. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

24. Plaintiff owns and operates computer systems that distribute third-party adult entertainment content. Plaintiff generates revenue by requiring third-parties to pay a fee for accessing its distributions systems. Members are assigned a username and password in order to access the distribution system.

25. Defendant obtained a username and password from a website that allows its members to trade stolen usernames and passwords amongst one another. Defendant used the stolen username and password to intentionally gain unauthorized access to Plaintiff's protected computer systems. Once Defendant gained unauthorized access to Plaintiff's protected computer systems, he permitted others to do the same.

26. Defendant accessed Plaintiff's computer systems as though he was a paying member. Defendant became privy to private information, including information regarding the identities of Plaintiff's customers, account information, financial information, computer programming and security information, and other information that Plaintiff protects and does not let third parties access to, even those who pay for and obtain legitimate passwords to access

Plaintiff's websites. Viewing such information not only inflicts harm to Plaintiff, but also potentially invades the privacy of those customers.

27. Since Defendant accessed the website through a hacked password, he was not required to provide any identifying personal information, such as his true name, address, telephone number or email address. Defendant can only be identified by his IP address.

28. Plaintiff identified the IP address associated with Defendant through computer software that allowed Plaintiff to detect the unauthorized breaches of its computer systems. The computer software detected the hacking, unauthorized access, and password sharing activity on Plaintiff's computer systems.

29. Once the IP address was ascertained, Plaintiff used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP address.

30. Plaintiff has suffered a loss due to the Defendant's fraud and abuse of Plaintiff's computer systems in excess of $250,000. The loss to Plaintiff includes, but is not limited to, 1) costs associated with detecting the unauthorized breaches and identifying the IP addresses of those associated, 2) costs associated with restoring its computer systems to their condition prior to the breach of its computer systems and preventing future breaches, and 3) lost revenue and costs incurred due to interruption of computer service.

31. Plaintiff has been damaged due to the Defendant's fraud and abuse of Plaintiff's computer systems in excess of $250,000. The damage to Plaintiff includes, but is not limited to, 1) harm to its business reputation by having its client and customer information accessed by unauthorized individuals, and 2) impairment to Plaintiff's computer systems made by changes to the systems caused by Defendant and his hacking program.

32. The above alleged facts support a claim of computer fraud and abuse by Plaintiff against Defendant under 18 U.S.C. § 1030.[2]

COUNT II – CIVIL CONSPIRACY

33. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

34. Defendant used a hacked username and password to gain access to Plaintiff's private systems. That access was based on an actual and/or implicit misrepresentation by Defendant that the hacked username and password actually authorized the Defendant to access Plaintiff's websites and systems.

35. Defendant, upon information and belief, belongs to a hacking community whose members share hacked usernames and passwords among other members. Members of this community work together to ensure that the members have access to normally inaccessible and unauthorized areas of the Internet.

36. By using and sharing hacked passwords and usernames, Defendant acted in concert with other members of this hacking community, and in a concerted action with other members, to accomplish unlawful transfers of Plaintiff's protected information.

37. Each time Defendant used a shared and hacked password and username, he reached an agreement with another co-conspirator(s) within the hacking community whereby the member provided the username and password in order to allow the Defendant to unlawfully access and obtain protected information from Plaintiff's websites.

38. Defendant had express or constructive knowledge that, in accomplishing the purposes of their common agreement, they were not acting unilaterally, and it was not fortuitous

[2] A private right of action exists under the Act under 18 U.S.C. § 1030(g).

or accidental that the Defendant performed acts in agreement with others for the purpose of misappropriating Plaintiff's protected systems.

39. Defendant understood the general objectives of the conspiratorial scheme, accepted them, and agreed, either explicitly or implicitly to do its part to further those objectives.

40. In furtherance of this civil conspiracy, Defendant committed overt tortious and unlawful acts by using hacked usernames and passwords to impermissibly obtain access to, and misappropriate private information from, Plaintiff's websites.

41. As a proximate result of this conspiracy, Plaintiff has been damaged, as is more fully alleged above.

JURY DEMAND

42. Plaintiff hereby demands a jury trial in this case.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays judgment and relief against Defendant as follows:

1) Judgment against Defendant that he or she has committed computer fraud and abuse against Plaintiff pursuant to 18 U.S.C. § 1030(g);

2) Judgment against Defendant's co-conspirators aided him/her in committing computer fraud and abuse against Plaintiff pursuant to 18 U.S.C. § 1030(g);

3) Judgment in favor of the Plaintiff against the Defendant for actual damages or statutory damages pursuant to 18 U.S.C. § 1030(g), at the election of Plaintiff, in an amount in excess of $100,000 to be ascertained at trial;

4) On Count II, an order that Defendant is jointly and severally liable to the Plaintiff in the full amount of Judgment on the basis of a common law claim for contributory infringement of copyright; for an award of compensatory damages in

favor of the Plaintiff and against Defendant, jointly and severally, in an amount to be determined at trial;

5) Judgment in favor of Plaintiff against the Defendant awarding the Plaintiff attorneys' fees, litigation expenses (including fees and costs of expert witnesses), and other costs of this action; and

6) Judgment in favor of the Plaintiff against Defendant, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted.

Respectfully submitted,

Guava LLC

DATED: October 5, 2012

By: s/ Michael K. Dugas

Michael K. Dugas
Bar No. 0392158
Attorney for Plaintiff
40 South 7th Street
Suite 212 – 307
Minneapolis, MN 55402
Telephone: (888) 588-9473
mkdugas@livewireholdings.com